A Report
to the
Montana
Legislature

Information Systems Audit

Achievement in Montana: Security of Student Information

Office of Public Instruction

February 2010

Legislative Audit
Division

09DP-10

Information Systems Audits

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. We conducted this IS audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objectives.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting, education, computer science, mathematics, political science, and public administration.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Direct comments or inquiries to:
Legislative Audit Division
Room 160, State Capitol
P.O. Box 201705
Helena, MT 59620-1705
(406) 444-3122

Reports can be found in electronic format at:
http://leg.mt.gov/audit

LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Monica Huyg, Legal Counsel

Deputy Legislative Auditors
James Gillett
Angie Grove

February 2010

The Legislative Audit Committee
of the Montana State Legislature:

We conducted an Information Systems audit of the Achievement in Montana (AIM) system which is a student information system. The Montana Office of Public Instruction (OPI) operates and maintains AIM to track student information required by federal regulations and to assist school districts with student record keeping. The focus of the audit was to ensure the security of student data in AIM. We reviewed user access controls and tested data processing and reporting controls to ensure data accuracy and integrity.

Overall, we found OPI has controls in place to ensure access to student data is limited and AIM is accurately processing and reporting student data. However, we did identify an area where OPI can improve, specifically relating to monitoring user accounts in AIM.

We wish to express our appreciation to personnel within the Office of Public Instruction for their cooperation and assistance.

Respectfully submitted,

/s/ Tori Hunthausen

Tori Hunthausen, CPA
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-Mail lad@mt.gov

TABLE OF CONTENTS

Figures and Tables

Figures

Appointed and Administrative Officials

Office of Public Instruction

Denise Juneau, Superintendent

Dennis Parman, Deputy Superintendent

Madalyn Quinlan, Chief of Staff

Susan Mohr, Administrator, Measurement and Accountability

Sara Loewen, AIM Unit Manager, Measurement and Accountability

REPORT SUMMARY

Achievement in Montana: Security of Student Information

In 2005, the 59th Montana Legislature defined a basic system of free quality public education that included the requirement to assess and track student achievement (20-9-309(2)(g), MCA). The legislature appropriated funding to the Office of Public Instruction (OPI) to develop and implement a statewide student achievement system that provides timely and accurate information about the performance of Montana's K-12 students and schools. In response, OPI implemented the Achievement in Montana (AIM) system to administer education information and support accountability at the local school districts and state level. This audit originated out of concerns about the security of a state controlled database containing personally identifiable student information.

AIM is designed to track a wide variety of student data including enrollment and demographics information. Montana school districts collect and store information on students in accordance with federal regulations such as the No Child Left Behind Act, Education Data Exchange Network reporting, and the Individuals with Disabilities Education Act (IDEA). There are also state requirements for data reporting, including calculation of average number belonging for school funding, registration for student assessment, and graduate and dropout rates. In AIM, local school district personnel enter each student's primary data just once. The data is then uploaded to the State Edition for reporting. A student's record contains the student's legal name, gender, birth data, race/ethnicity, and types of educational services received. Additional information includes:

- Scores on statewide assessments
- Information for determining a school's "Adequate Yearly Progress" (AYP)
- Student dropout information
- Information needed for serving students with disabilities
- Participation in federal and state grant programs

The primary focus of this audit was to ensure the security of student data from the input process at the district level, to the reporting and analysis processes performed by OPI. AIM is critical to OPI's ability to maintain and report Montana student data. As such, it is imperative the system is completely storing, processing, and reporting student data.

Based on our work, we conclude OPI has successfully implemented a statewide student information system. We identified system and security controls in place to maintain AIM data security and integrity. We reviewed controls over data entry to ensure consistency of data, as well as delivered processing controls ensuring AIM data validity. We reconstructed baseline reports and compared the output with delivered reporting functionality to ensure AIM is generating accurate reports. While controls are in place, we identified areas in the management of user accounts in AIM where OPI could improve. Specifically, OPI should establish procedures for reviewing all user accounts and related privileges in the State Edition of AIM.

Chapter I – Introduction and Background

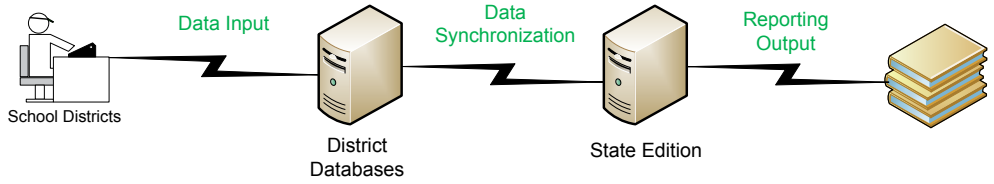
Introduction

In 2005, the 59th Montana Legislature defined a basic system of free quality public education that included the requirement to assess and track student achievement (20-9-309(2)(g), MCA). The legislature appropriated funding to the Office of Public Instruction (OPI) to develop and implement a statewide student achievement system that provides timely and accurate information about the performance of Montana's K-12 students and schools. In response, OPI implemented the Achievement in Montana (AIM) system to administer education information and support accountability at the local school districts and state level. This audit originated out of concerns about the security of a state controlled database containing personally identifiable student information.

Background

In June 2006, OPI contracted with a third-party vendor of student information software. As part of the agreement, the vendor customized an off-the-shelf package for use by OPI called the State Edition. The State Edition of AIM collects student data needed for OPI to meet state and federal reporting requirements. The system is designed to synchronize district data with the State Edition. This automated synchronization of student data occurs as it is entered at the district level. The following figure shows the flow of data through AIM.

Figure 1
AIM Data Flow



Source: Compiled by the Legislative Audit Division.

AIM is designed to track a wide variety of student data including enrollment and demographics information. Montana school districts collect and store information on students in accordance with federal regulations such as the No Child Left Behind Act, Education Data Exchange Network reporting, and the Individuals with Disabilities Education Act (IDEA). There are also state requirements for data reporting, including

calculation of average number belonging for school funding, registration for student assessment, and graduation and dropout rates. In AIM, local school district personnel enter each student's primary data just once. The data is then uploaded to the State Edition for reporting. A student's record contains the student's legal name, gender, birth date, race/ethnicity, and types of educational services received. Additional information includes:

- Scores on statewide assessments
- Information for determining a school's "Adequate Yearly Progress" (AYP)
- Student dropout information
- Information needed for serving students with disabilities
- Participation in federal and state grant programs

Audit Objectives

The audit objectives were developed based on our analysis of risk over the security of Montana student information housed in AIM. The primary focus was to ensure the security of student data from the input process at the district level, to the reporting and analysis processes performed by OPI. AIM is critical to OPI's ability to maintain and report Montana student data. As such, it is imperative the system is completely storing, processing, and reporting student data. Due to the critical role of the system, we conducted audit work to address the following four objectives:

1. Verify controls are in place to ensure the availability of real time data in AIM.
2. Ensure controls are in place to prevent unauthorized access to student data in AIM.
3. Verify processing controls are in place to ensure AIM data completeness.
4. Ensure AIM is generating accurate reports.

Audit Scope and Methodology

The main consideration regarding scope was the multiple edition design of AIM. This design puts the responsibility of data input with the data owners: the individual school districts. The scope of this audit was limited to review of data, processing, and reporting in only the State Edition of AIM. Audit verification of data integrity and security consists of reviewing controls over student data in AIM. Audit work also included review of system-generated reports to ensure data accuracy and completeness.

The methodology used in this audit included interview of OPI staff and district representatives, query and analysis of AIM data, review of OPI and system-related documentation, and observation of AIM operations. This audit was conducted in accordance with Government Auditing Standards published by the United States

Government Accountability Office (GAO). We evaluated the control environment using best practices and generally applicable and accepted information technology standards established by the IT Governance Institute.

Audit Overview

Based on our work, we conclude OPI has successfully implemented a statewide student information system. We identified system and security controls in place to maintain AIM data security and integrity. We reviewed controls over data entry to ensure consistency of data, as well as delivered processing controls ensuring AIM data validity. We reconstructed baseline reports and compared the output with delivered reporting functionality to ensure AIM is generating accurate reports. While controls are in place, we identified areas in the management of user accounts in AIM where OPI could improve. Specifically, OPI should establish procedures for reviewing all user accounts and related privileges in the State Edition of AIM. The remainder of this report discusses our findings and recommendations.

Chapter II – Student Data Security and Integrity

Introduction

In order for the Office of Public Instruction (OPI) to report student information, it needs student data from all of Montana's school districts. OPI uses the State Edition of the Achievement in Montana (AIM) system to fulfill reporting requirements. System and security controls over AIM ensure the integrity of student data, business processes, and reports generated from the system. These controls include data entry controls, student data synchronization, change management procedures, logical access controls, and reporting controls. This chapter discusses our findings related to ensuring student data security and integrity in AIM.

Data Entry Controls

OPI relies on data reported from the districts to populate the State Edition of AIM. There are baseline data entry controls in place to help ensure student data integrity. These controls include system edits automatically run during the data entry process. One control during data entry temporarily halts processing while prompting a user for correction or confirmation of submitted data. The edits halt data entry due to missing data, incorrect data types, or when updating already existing student data. Testing of these edits confirmed they ensure the minimum required information is included during data entry and prompt for user confirmation when overwriting existing data.

Student Data Synchronization

We reviewed the process in place to transfer information to OPI. The main process used to ensure data is reported completely to OPI is student data synchronization from the districts to the State Edition of AIM. Our review of the automated synchronization process verified a documented process is in place. Audit work was performed to confirm the synchronization process is working as intended.

OPI staff generate and review reports of student information in the State Edition of AIM on a daily basis. Reports are analyzed to ensure student data is consistent, and all data OPI needs for reporting purposes is complete and up to date. OPI staff review reports to check for duplicate students, enrollment data, dropouts, and graduates. To verify the synchronization process ensures complete data transfer, audit work compared student records from the districts with the student data in the State Edition of AIM. This analysis determined the data in the State Edition has completely transferred from the districts to OPI.

Conclusion

Based on our work, we conclude data entry controls are in place to ensure the integrity of data being entered into AIM. Audit work verified there are controls in place to ensure student data is completely transferred from districts to the State Edition of AIM.

Change Management Controls

While OPI has controls in place to ensure accurate student data is reported from the districts to the State Edition of AIM, we performed additional work to verify the State Edition is accurately processing and storing the data. To confirm AIM is operating as expected, we reviewed change management controls over the State Edition of AIM. Change management controls require specific procedures during development and modification of AIM functionality. The documented process in place for all change requests includes submission of a request, review of suggested changes and analysis of potential impacts, testing, management review and approval, and finally implementation.

The programming code for AIM is proprietary to the vendor. As such, all changes to AIM are developed by the vendor and provided to OPI as updated versions or patches to AIM, which are then tested and approved by OPI before implementation. Audit work reviewed the change management process and confirmed it is working as intended.

Conclusion

Based on our work, we conclude change management procedures are in place to ensure changes are tested and authorized before being implemented in the State Edition of AIM.

User Access Controls

Although we identified controls over data entered into AIM, there is additional risk that system data can be inappropriately modified by someone with access to the system. As a result, we reviewed user access controls. Our first step was to verify OPI has implemented a process to grant access to AIM. We noted OPI has created a form where access requests and management authorization are documented. We reviewed a sample of forms and determined the access request process is being followed.

OPI policy is to limit access to AIM through least privilege, granting a user only enough access to perform their job duties. Approved access request forms are maintained by OPI's security officer. There are two types of access controls in AIM: the first is user groups, which grant rights to functionality; the second is calendars, which are structures used to organize student information by school.

User groups are combinations of access to different screens and functionality in AIM, which determine what information a user can access and what a user can do, including the ability to view, modify, add, or delete data. These user groups can be created to grant or limit specific access to various aspects of AIM. Audit work reviewed State Edition user group access, based on job duties assigned to all users including OPI staff and school district personnel. Review of user access in AIM determined district users are limited to appropriate group access and OPI staff user access is segregated by least privilege.

The second control regulating access to student information in AIM is calendars. In AIM, students are added into a calendar specific to the school in which the student is currently enrolled. Since students are associated with their school calendar, OPI uses this to segregate access to student information. This means that while AIM stores all student information in a single database, users can only view student information in the school or school district calendars they are assigned to. Audit work was performed reviewing calendar access for accounts in the State Edition of AIM. Review of calendar access assigned to OPI user accounts determined access is appropriate to their job duties, and district user accounts only have access to calendars for their respective district.

Conclusion

Audit work determined OPI has implemented a policy of least privilege when assigning access to users in the State Edition of AIM, and has controls to limit access to AIM functionality and student records based on job duty.

District User Access

According to the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. §1232g), only authorized individuals with a legitimate educational interest should have access to student data. This federal law is intended to protect personally identifiable information and applies to all schools receiving funds under an applicable program of the U.S. Department of Education. OPI has established policies regarding student record confidentiality and information technology acceptable use. In addition, all

users are required to sign a confidentiality statement when requesting access to AIM. While district accounts are restricted to view access and limited to associated student information, we reviewed district user access to the State Edition of AIM to ensure it is controlled.

We noted district users have access to the State Edition of AIM via an account assigned to a district authorized representative, which is the district superintendent by default. According to OPI, this access is granted so school districts can confirm the accuracy of transferred data. At the time of our audit there were 435 of these accounts in use.

The responsibility for ensuring the accuracy of student data in the State Edition of AIM requires work by district personnel. The amount of work required will fluctuate according to the number of records reviewed. Because the district authorized representative may not be able to complete all required reviews without assistance, the potential for sharing district accounts increases. If district accounts are shared, individual accountability is compromised. This situation could potentially allow unauthorized individuals to view student information.

In order to determine the extent of district use of the State Edition of AIM, we contacted a judgmental sample of district users. Our sample was selected based on usage information logged within AIM. Results of our calls indicated a lack of awareness and understanding of uses of district accounts. We noted some users at smaller schools indicated they did not know they were responsible for confirming student data in the State Edition of AIM. As such, these users had not logged into the State Edition of AIM since their initial training. In addition, the authorized user at one of the smaller schools we called was no longer employed by the district. At the larger school districts we called, we were informed multiple users log into the State Edition of AIM to confirm the accuracy of student data. In these instances, multiple individuals share the single district account in order to log onto the State Edition of AIM. Due to the high number of students in the larger districts, users said it is difficult for a single user to confirm the accuracy of transmitted student data. The existence of multiple users sharing a single account increases the possibility that users have not been properly authorized to view sensitive student data, which conflicts with OPI policy and federal regulations regarding confidentiality of student records. In addition, there appears to be a need for training regarding adherence to policy and use of the State Edition of AIM.

During our review of district user access, we noted the access log in the State Edition of AIM indicated some users had not changed the password for the district account since its creation. OPI policy on acceptable use require users to change their passwords

at least every 60 days. In addition, users requesting access to AIM, including district authorized representatives, are required to sign a confidentiality statement, which references related OPI policies.

According to Control Objectives for Information and related Technologies (COBIT), user accounts and related user privileges should be regularly reviewed by management. District personnel have access to the State Edition of AIM, but current practices for assignment of district accounts do not include ongoing account management as suggested by industry standards. OPI has policies regarding acceptable use; however, these policies are not being followed. Users are sharing accounts, not updating passwords, and current account assignments are not up to date, which results in lack of individual accountability. As such, OPI cannot ensure only appropriate individuals access student information in the State Edition of AIM. In addition, some district users indicated they were not aware of the need for conducting data confirmation activities. As a result, our findings indicate a need for improved district account management.

RECOMMENDATION #1

We recommend the Office of Public Instruction:

A. *Establish procedures to require unique accounts for all district users.*

B. *Establish account management procedures to ensure district account user information is up-to-date and all users comply with applicable policies.*

C. *Ensure district users receive appropriate training regarding security of student data and use of the system.*

Reporting Controls

AIM must have the ability to generate accurate and reliable data related to student demographics, student achievement, and other information requested by OPI, the Montana Legislature, and the U.S. Department of Education. In order to ensure accurate and reliable data is being reported by AIM, we reviewed controls in place over delivered and custom reporting. Audit work included comparative analysis between data in the database and data from delivered and custom generated reports. The controls and policy related to modifications of baseline reports were found to be consistent with our findings on change management.

With the assistance of OPI, we selected a judgmental sample of enrollment reports and created an extract of student data directly from the State Edition of AIM. We then

generated delivered reports, as well as OPI created ad-hoc reports, covering the same data sets as in our sample. Our comparative analysis of baseline data against delivered and custom ad-hoc reports resulted in a 100 percent match in reported data.

CONCLUSION

Based on audit work, we conclude reports included in our sample are accurately reporting student data from AIM.

Office Response

OFFICE OF PUBLIC INSTRUCTION
STATE OF MONTANA

Denise Juneau
Superintendent

www.opi.mt.gov
(406) 444-5643

February 12, 2010

RECEIVED
FEB 12 2010
LEGISLATIVE AUDIT DIV.

Tori Hunthausen, Legislative Auditor
Legislative Audit Division
Room 135, State Capitol
P.O. Box 201705
Helena, MT 59620-1705

Dear Ms. Hunthausen:

The purpose of this letter is to provide comments by the Office of Public Instruction (OPI) concerning the Information System's audit of the Achievement in Montana system. We thank Kent Rice, Stephen Daem, and Nathan Tobin for their hard work and professionalism in this audit. The following is our response to the recommendations in the information systems audit.

Recommendation #1
We recommend the Office of Public Instruction:

A. Establish procedures to require unique accounts for all district users.

OPI Response: We concur. The OPI agrees that, in order to improve control over access to the AIM State Edition system, unique accounts for district personnel must be established. The establishment of unique accounts will dramatically increase the number of accounts the agency will be required to create and manage. In order to effectively control the additional accounts, the OPI recognizes that it needs an automated system that will allow the districts a certain degree of self service and also provide an easy and effective way to audit the access to the AIM State Edition.

The OPI has been investigating a third party identity management solution that will offer the increased control and monitoring needed to manage the proposed increase in accounts. We believe identity management solution will allow the agency to require unique accounts for all users in the districts as well as put in place the processes and procedures required to effectively manage the increased number of accounts. The current plan is to purchase the solution and have it installed by fall of 2010.

B. Establish account management procedures to ensure district account user information is up-to-date and all users comply with applicable policies.

OPI Response: We concur. The identity management solution referred to in response #1A will provide the tools needed to both enforce certain policies and monitor compliance. For instance,

the tool can enforce password resets on a regular basis and insure passwords follow the agency's policy on length and composition. The identity management solution can also be configured to allow regular audits to ensure that user information is up-to-date. Depending on the final implementation decisions, districts can be required to validate their authorized accounts on a re-occurring basis and certify that the accounts that have access have rights appropriate to their job duties.

C. Ensure district users receive appropriate training regarding security of student data and use of the system.

OPI Response: We concur. The success of an effective identity management system is contingent on the users of the system, in this case, schools and districts, embracing and using the system. The OPI requires all agency staff to receive training on the confidentiality policy with respect to student records. Annual confidentiality refresher training is provided to those OPI staff members who interact with school district personnel to ensure the security measures and confidentiality of student data is followed.

OPI AIM staff members conduct regional fall trainings for school and district personnel. At these trainings, the AIM staff will emphasize and address the confidentiality and security requirements of student data. Training will also be provided on the new identity management system (once that system has been installed at the OPI).

In addition, the OPI has produced three web-based presentations regarding the security of student data. These presentations can be found on the OPI web page at: http://www.opi.mt.gov/Reports&Data/AIM/Index.html#gpm1_11 . The topics include OPI Student Records Confidentiality and Security, School District Responsibilities and Features of AIM, and Technology and Infrastructure for AIM. OPI uses these presentations in its agency-wide training and will continue to promote these presentations to school personnel and anyone else interested in understanding OPI's student records confidentiality policies and practices.

Thank you for the opportunity to comment on this information systems audit report. We are enthusiastic in our plans to implement the recommendations of this report.

Sincerely,

Denise Juneau
Superintendent of Public Instruction